P102812RR (2)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/30 — A1

(11) International Publication Number: **WO 99/40742**

(43) International Publication Date: 12 August 1999 (12.08.99)

(21) International Application Number: PCT/FI99/00079

(22) International Filing Date: 3 February 1999 (03.02.99)

(30) Priority Data:
980254 4 February 1998 (04.02.98) FI

(71) Applicant *(for all designated States except US)*: NOKIA TELECOMMUNICATIONS OY [FI/FI]; Keilalahdentie 4, FIN–02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: PYYHKÄLÄ, Jouni [FI/FI]; Terhokuja 4 B 7, FIN–01710 Vantaa (FI).

(74) Agent: PATENT AGENCY COMPATENT LTD.; P.O. Box 156, FIN–00511 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

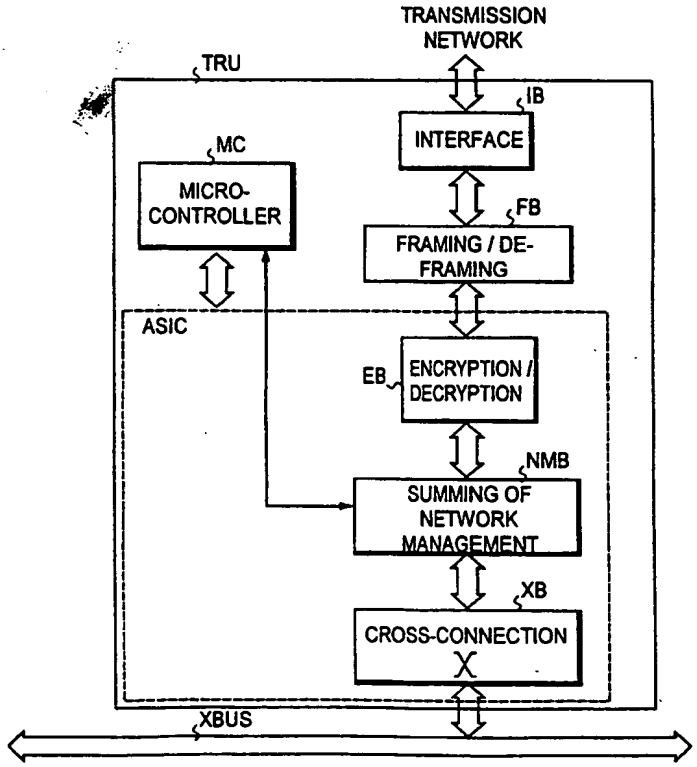
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

In English translation (filed in Finnish).

(54) Title: DATA TRANSMISSION METHOD WITH ENCRYPTION PERFORMED IN AN INTERNAL CARD UNIT (TRU)

(57) Abstract

The invention concerns implementation of data transmission in a mobile network including base transceiver stations (BTS) forming radio cells, mobile stations (MS) located in the areas of the radio cells and being in connection with the base transceiver stations over a radio path, and at least one base station controller (BSC), which through a transmission network is in connection with the base transceiver stations. In at least a part of the transmission network data is transmitted in an encrypted form. In order to achieve good data security in the transmission network and in order to achieve as easy processing as possible of the signals of the transmission network, the encryption is carried out in an internal card unit (TRU) of the base tansceiver station before framing of the bit flow to be transmitted to the transmission network.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Data transmission method with encryption performed in an internal card unit (TRU)

Field of the invention

The invention relates generally to data transmission taking place in a mobile network, more specifically to data transmission implemented in the fixed part of a mobile network. In this context, the fixed part means that part of the mobile network which extends in the uplink direction of the transmission link from the base transceiver stations, especially connections between the base station controller and a base transceiver station or between two successive base transceiver stations. Although the network is called a fixed network in this context, it should be noted that this fixed network or its part can be implemented e.g. with the aid of radio links.

Background of the invention

To illustrate the typical architecture of a mobile network, Figure 1 shows the structure of the known GSM mobile communications system (Global System for Mobile Communications), using abbreviations known from the context of the GSM system. The system comprises several open interfaces. The transactions relating to crossing of interfaces have been defined in the standards, in which context the operations to be carried out between the interfaces have also been largely defined. The network subsystem (NSS) of the GSM system comprises a mobile services switching center (MSC) through whose system interface the mobile network is connected to other networks, such as a public switched telephone network (PSTN), an integrated services digital network (ISDN), other mobile networks (Public Land Mobile Networks PLMN), and packet switched public data networks (PSPDN) and circuit switched public data networks (CSPDN). The network subsystem is connected across the A interface to a base station subsystem (BSS) comprising base station controllers (BSC), each controlling the base transceiver stations (BTS) connected to them through a transmission network. The interface between the base station controller and the base stations connected thereto is the Abis interface. The base stations, on the other hand, are in radio communication with mobile stations MS across the radio interface.

The GSM network is adapted to other networks by means of the interworking function (IWF) of the mobile services switching center. On the other hand, the mobile services switching center is connected to the base station

controllers with PCM trunk lines crossing the A interface. The tasks of the mobile services switching center include call control, control of the base station system, handling of charging and statistical data, and signalling in the direction of the A interface and the system interface.

The tasks of the base station controller include, inter alia, the selection of the radio channel between the controller and a mobile station MS. For selecting the channel, the base station controller must have information on the radio channels and the interference levels on the idle channels. The base station controller performs mapping from the radio channel onto the PCM time slot of the link between the base station and the base station controller (i.e., onto a channel of the link).

The base station controller BSC includes trunk interfaces, by which it is connected on the one hand to the mobile services switching center over the A interface and on the other hand to the base transceiver stations over the Abis interface. The transcoder and rate adaptation unit TRAU forms part of the base station system and may be incorporated into the base station controller or the mobile services switching center. The transcoders convert speech from a digital format to another, for example convert the 64 kbit/s PCM signals arriving from the mobile services switching center across the A interface into 13 kbit/s coded speech signals to be conveyed to the base station, and vice versa. Data rate adaptation is performed between the speed 64 kbit/s and the speed 3.6, 6, or 12 kbit/s. In a data application, the data does not pass through the transcoder.

The base station controller configures, allocates and controls the downlink circuits. It also controls the switching circuits of the base station via a PCM signalling link, thus enabling effective utilization of PCM time slots. In other words, a branching unit at a base station, which is controlled by the base station controller, connects the transmitter/receivers to PCM links. Said branching unit transfers the content of a PCM time slot to the transmitter (or forwards it to the other base stations if the base stations are chained) and adds the content of the receive time slot to the PCM time slot in the reverse transmission direction. Hence, the base station controller establishes and releases the connections for the mobile station.

The layer 1 physical interface between the base station BTS and the base station controller BSC is in this example a 2048 kbit/s PCM line, i.e. comprises 32 64 kbit/s time slots (= 2048 kbit/s). The base stations are fully

under the control of the base station controller. The base stations mainly comprise transmitter/receivers providing a radio interface towards the mobile station. Four full-rate traffic channels arriving via the radio interface can be multiplexed into one 64 kbit/s PCM channel between the base station controller and the base station, and hence the speed of one speech/data channel over this link is 16 kbit/s. Hence, one 64 kbit/s PCM link may transfer four speech/data connections.

Figure 1 also shows the transfer rates used in the GSM system. The mobile station MS transmits speech data across the radio interface on the radio channel for example at the standard rate 13 kbit/s. The base station receives the data of the traffic channel and switches it to the 64 kbit/s time slot of the PCM link. Three other traffic channels of the same carrier are also located in the same time slot (i.e., channel), and hence the transfer rate per connection is 16 kbit/s, as stated previously. The transcoder/rate adaptation unit TRAU converts the encoded digital information to the rate 64 kbit/s, and at this rate the data is transferred to the mobile services switching center. If the transcoder/rate adaptation unit is incorporated into the mobile services switching center, maximum advantage is gained from compressed speech in data transmission.

In the latest solutions, base transceiver stations are chained in the manner shown by Figure 2, one after the other in such a way that each base transceiver station will take from the transmission network the traffic of the time slots allocated for its own (card) units and will switch the remaining time slots to the next base transceiver station. Hereby there is within one card unit of the base transceiver station (or between two different card units) a fixedly defined branch for branching the traffic to the base transceiver station which is next in the chain. In Figure 2, the first base transceiver station after the base station controller branches the traffic arriving from the base station controller into three different chains, and in each chain each base transceiver station will then receive the data of those time slots, which are intended for its own units and will switch the data of other time slots forward in the chain. In the figure the reference mark TRU is used to indicate these transmission units carrying out the branching. Using an additional unit (DMR) it is also possible to form e.g. a radio link connection between base transceiver stations. In this example, the base station controller is connected through a separate cross-connection de-

vice XD to a first base transceiver station, wherein the arriving traffic is branched to three separate base transceiver station chains.

In that part of the network which is in the uplink transmission direction from the base transceiver stations, the traffic, however, usually goes unencrypted from one network element to another. In the network part between base station controllers and base transceiver stations in particular it is hereby relatively easy to follow the traffic in the network, either the whole data flow or one or more individual time slots, e.g. a network management channel.

In such network environments where data security is of special importance, encrypting of the data to be transmitted is performed when required also in the network part between base transceiver stations and base station controllers. This is carried out in such a way that to one or more legs where encryption of data is desired such devices are added which at the transmission end perform encryption of the data to be transmitted to the link and at the reception end perform decryption before the data is received. The devices are located outside the transmission equipment (e.g. the base transceiver station) proper.

A drawback of such a solution is that it is difficult to process the encrypted data flow, if e.g. it is transmitted from one system to another (e.g. if PCM signals are transmitted to a SDH (Synchronous Digital Hierarchy) system, between network parts owned by two separate operators or even just between two such pieces of transmission equipment, which have different transmission capacities. In practice the data must in fact always first be decrypted, in order to reveal the standard signal format for processing.

Summary of the invention

It is a purpose of the invention to eliminate the drawback described above and to bring about a method, using which it is possible to implement data security in a mobile network in such a way that processing of signals remains as simple as without encryption.

This objective is attained by the solution defined in the independent claims.

The idea of the invention is to perform data encryption in a card unit within the base transceiver station before framing of the data flow to be transmitted to the transmission network and, correspondingly, to perform decryption only after the frame structure of the received data has been disassembled and

the payload data has been separated from the frame information. In this way encryption can be performed without breaking against the requirements or provisions needed by the external interface of the network element, and preserving the standard signal format, whereby the signal can also be processed outside the base transceiver station in as simple a way as when processing an unencrypted signal.

The network management channel is summed into the data stream to be transmitted before the encryption, so it is encrypted along with the other data. Thus no one else but the network operator can read or change the settings of network elements or their units in the network. In this way it is possible to prevent any paralysis of parts of the network or any momentary taking over of the network or its part for use by another operator.

Not only does encryption make it more difficult to eavesdrop channels but it also makes it more difficult e.g. for a competing operator to perform any monitoring of traffic volumes transmitted through the network. This is due to the fact that after encryption one can no longer tell on which channel there is traffic and on which there is none, because the bit pattern also of unused time slots will change as a result of the encryption.

List of figures

In the following the invention and its advantageous modes of embodiment will be described in greater detail referring to Figures 3 and 4 in the examples according to the appended drawings, wherein

Figure 1 illustrates the structure of a GSM mobile network;
Figure 2 shows base transceiver stations chained one after the other;
Figure 3 illustrates the typical architecture of a base transceiver station; and
Figure 4 illustrates a solution in accordance with the invention at a transmission unit of a base transceiver station.

Detailed description of the invention

The architecture of a base transceiver station is typically such as shown in Figure 3, that is, such that on the backplane BP or mother board of the base transceiver station those internal buses INB of the equipment are implemented, to which the card units of the base transceiver station are connected (card units are also called plug-in units). The card units of the base

transceiver station are typically transmission units and base transceiver station units. The transmission unit attends to the traffic between the transmission network and the base transceiver station and an external interface of the base transceiver station is formed therein for the transmission network. The base transceiver station unit for its part contains the base transceiver station's radio parts, which are connected to an antenna. The figure shows two base transceiver station units and they are marked with the reference marks BSU1 and BSU2. The number of transmission card units is also two and they are marked with the reference marks TRU1 and TRU2. The number of transmission card units may vary and they may be equipped with access interfaces of many types. The transmission card units may also provide e.g. HDSL or ISDN interfaces. Such interfaces are formed in the example shown in the figure through the front connectors (FC1 and FC2) of the transmission card units .

Figure 4 illustrates the solution according to the invention in a base transceiver station of a cellular network. Since the encryption method according to the invention is implemented explicitly on the transmission card unit of the base transceiver station, the figure shows only one transmission card unit TRU of these card units of the base transceiver station. It is assumed in the example that a 2048 kbit/s PCM line is connected to the interface of the transmission card unit. Thus the interface towards the transmission network is in compliance with the recommendations of CCITT's (nowadays ITU-T) G.700 series.

In the transmission card unit there is first in the reception direction an interface block IB, where synchronization takes place with the incoming signal and where the line-coded signal (e.g. three-level HDB3 coding used on PCM lines) is changed into binary data. In the transmission direction the same actions are performed in the opposite order, that is, the signal to be transmitted is adapted physically to the transmission path.

From the interface block the data stream is switched in the reception direction to a framing block FB, where the frame structure of the signal to be received is disassembled. In other words, the useful data is separated from the frame information. In the transmission direction a frame structure to be transmitted is formed in the framing block for the interface from the bit stream to be transmitted (those bits are added to the data flow, which belong solely to the frame structure, e.g. the frame alignment bits).

In the reception direction the bit string to be received is then decrypted in the encryption/decryption block EB. In the transmission direction encryption of the bit string to be transmitted is correspondingly performed in this block. The encryption may be performed by any method known as such, which provides a data security level which is sufficient for the environment in question. However, it is preferable to use such an encryption method, which will produce a bit string of equal length directly from the original bit string. However, it is also possible to use a solution, wherein the encrypted bit string resulting from the original bit string is shorter than the original. In such a case "stuffing bits" must be added to the encrypted bit string before the data is framed. It is also possible in principle to use such an encryption algorithm, which makes the encrypted bit string longer than the original, but this is the poorest alternative in the sense that the payload data capacity will be reduced. Encryption is preferably done in the bit flow on such a bit string, the integrity of which is known to remain over the transmission path.

In the reception direction after the encryption block the bit flow is switched to the network management block NMB, where the network management data contained in the bit flow is separated from the bit flow for the microcontroller MC of the card unit. Correspondingly, in the transmission direction the network management bits are summed under control by the microcontroller into the bit flow to be transmitted. (In practice, almost every card unit has its own controller, which controls the functions of the card unit.)

To the other received time slots cross connection is performed in the cross-connection block XB, which is connected to the cross-connection bus XBUS (which is a part of the bus system INB on the backplane of the base transceiver station) between the units. In the cross-connection unit some time slots are connected to the radio unit of the own base transceiver station while some are connected to such interfaces, which are connected through the transmission path to other base transceiver stations. One or more such interface may also be in the same transmission card unit, because one transmission card unit may have more than one interface. Correspondingly, in the transmission direction the cross-connection block is used to connect the contents of the base transceiver station's reception time slots or the contents of time slots received from other base transceiver stations to the correct time slots of the PCM signal to be transmitted from the desired interface.

Since the encryption and decryption are carried out in a manner known as such, it will not be described in greater detail in this connection. What is essential from the viewpoint of the invention is that the encryption and decryption are performed within the transmission card unit of the base transceiver station between the cross connection performed by the card unit and the de-framing/framing. E.g. as seen in the reception direction, the place is that where the bit flow received from the transmission network is processed unframed and that place which is located in the reception direction before the data is connected forward to the other units, preferably before bits are separated from the data even for use by the same transmission card unit. Correspondingly, in the transmission direction the preferable place is that where all information has already been summed into the bit flow to be transmitted, but where the bit flow is still in the form of unframed binary data.

Figure 4 shows functional blocks contained in the transmission card unit TRU. The manner in which these blocks are located in physical circuits may vary in many ways. E.g. it is possible in practice to perform in the same circuit the implementation of the physical interface and the framing/de-framing. On the other hand, the blocks described above may be located in one customer circuit (application-specific integrated circuit), e.g. in such a way that the circuit includes all other blocks except the interface or the interface and the framing block. Thus the functional blocks described above can be integrated within one or more circuits. In addition, one circuit may have certain functions for more than one transmission connection, e.g. there may be several interfaces in one line circuit. However, there are specific functional blocks for each interface.

The encryption is preferably carried out on every leg of the network part between the base station controller and the base transceiver stations, so encryption may be performed not only in the base transceiver stations of Figure 1 but also in the base station controller BSC and/or in the cross-connection device XD. But when moving from the base station controller towards the mobile services switching center, the capacities of transmission connections usually become so high that an optical fiber is used as transmission medium in most cases. Hereby the same benefit can not be derived from encryption, since it is anyway difficult to eavesdrop an optical fiber.

Decryption is always performed in the following network element containing the cross-connection of the same operator, so that multiple encryp-

tion will not result. If there are pieces of transmission equipment of another operator in between, no decryption need be done in these, because the signal can be processed in exactly the same manner as a normal non-encrypted signal travelling in the network.

Encryption may be carried out using a fixed encryption key, or the encryption key may be changed when desired. If it is desired to change the encryption keys constantly, this must be taken into account when the network capacity is determined. In other words, of the transmission capacity a part must be reserved for the transmission of encryption keys and/or synchronization information of the encryption. The network management may inform the base transceiver stations both about encryption keys and about the moment of their change or only about the moment of change, if the new encryption key is already known to the base transceiver station. Since the traffic must run constantly and since it is not desirable that at the moment of encryption key change a non-encrypted mode exists for a moment, the base transceiver stations must be mutually synchronized so that they will change the encryption key at the right moment. For conveying this synchronization information one bit of the frame is sufficient, which bit may be conveyed e.g. in time slot TS0, if the signal is a 2048 kbit/s signal in accordance with ITU-T's G.703/G.704 recommendations (in every second frame there is a frame alignment character in the TS0 time slot, but in every second bits 4-8 are free for national use, whereby they may be used for transmission of synchronization information). For the synchronization information, bits may also be reserved from some other time slot, but hereby the necessary capacity must be taken from the capacity reserved for the payload.

New encryption keys may be conveyed e.g. on the network management channel (e.g. time slot TS16 of a 2048 kbit/s signal). The base transceiver station may also have an encryption key database, wherein all encryption keys available to the base transceiver station are stored beforehand, e.g. when the network element is installed. Hereby no more than the above-mentioned synchronization information is sent from the network management system to inform when the encryption key is exchanged. The base transceiver stations may also count frames and change the encryption key e.g. always after a certain number of frames.

One base transceiver station may use several different encryption keys at the same time, since several transmission connections may start out from one base transceiver station.

Owing to the solution in accordance with the invention, a data flow can be transmitted e.g. in leased links in a very simple manner without the owner of the links being able to find out the content of the data flow. Seen from outside the data flow appears to be a normal transmission connection and it meets the provisions of the standard. Thus it is possible to handle the data flow, e.g. transmit it between the own equipment and the lessor's equipment without having to take any additional steps due to encryption.

Although the invention was described above referring to the examples shown in the appended drawings, it is obvious that the invention is not limited to these, but it can be modified within the scope of the inventive idea presented in the appended claims. Also other data than mobile network traffic may be transmitted in the network. Although encryption of a bit flow is mentioned in this connection, it is possible in the encryption block also to use a data scrambler, if the data security provided by this is sufficient in practice. However, when using a data scrambler the same level of data security is not achieved as when using encryption based on a key. However, the term "encryption" must be construed as meaning all the different alternatives, by which the data flow is changed into an unintelligible form. Nor is it necessary to perform cross connection in the base transceiver station in the manner described above (e.g. a base transceiver station located at the end of a chain). An individual interface may also be unidirectional, whereby only encryption or decryption is performed in it. It should also be noted that when the appended claims mention units of a base transceiver station, one unit does not necessarily correspond to one card unit, but a unit may be distributed to several card units or one card unit may have several units or parts of more than one unit.

Claims

1. Method of implementing data transmission in a mobile network including

- base transceiver stations (BTS) forming radio cells,
- mobile stations (MS), which are located in the areas of the radio cells and which are in connection with the base transceiver stations through a radio path, and
- at least one base station controller (BSC), which through a transmission network is in connection with the base transceiver stations, according to which method data is transmitted in an encrypted form in at least a part of the transmission network,

characterized in that the encryption is performed in an internal card unit (TRU) of the base transceiver station before framing of the bit stream to be transmitted to the transmission network.

2. Method as defined in claim 1, characterized in that in the said internal card unit decryption is also performed of the data received from the transmission network, and that the decryption is performed after the deframing of the frame structure of the received signal.

3. Method as defined in claim 2, characterized in that network management information is added to the data to be transmitted before encryption of the data to be transmitted.

4. Method as defined in claim 2, characterized in that encryption is used on every link starting out from an individual base transceiver station towards the base station controller.

5. Method as defined in claim 4, characterized in that decryption is always performed in that next network element possessed by the same operator, wherein cross connection is performed.

6. Method as defined in claim 1, characterized in that the encryption uses an encryption key, which is changed at certain intervals of time.

7. Method as defined in claim 6, characterized in that the encryption keys used are transmitted to the base transceiver stations through the transmission network.

8. Method as defined in claim 6, characterized in that the change of encryption key is synchronized through the transmission network.

9. Base transceiver station of a mobile network, which by way of a radio path is in connection with mobile stations (MS) located in the area of a cell formed by the base transceiver station and through a transmission network with means (MSC) controlling the base transceiver station, which base transceiver station includes

- at least one transmission unit (TRU), which forms at least one interface (IB) towards the transmission network,
- at least one unit, which forms a radio interface towards the mobile stations (MS), and
- an internal bus system (INB) including several buses to which the units are connected and with the aid of which the units are in connection with one another,

whereby framing means (FB) pertain to at least one individual interface for framing the data flow to be transmitted before its transmission through the interface to the transmission network,

characterized in that

- the transmission unit (TRU) also includes encryption means (EB) for encryption of the data to be transmitted to the interface, said means being located so that in the transmission direction they are located before the said framing means.

10. Base transceiver station of a mobile network, which by way of a radio path is in connection with mobile stations (MS) located in the area of a cell formed by the base transceiver station and through a transmission network with means (MSC) controlling the base transceiver station, which base transceiver station includes

- at least one transmission unit (TRU), which forms at least one interface (IB) towards the transmission network,
- at least one unit forming a radio interface towards the mobile stations (MS), and
- an internal bus system (INB) including several buses, to which the units are connected and with the aid of which the units are in connection with one another,

whereby de-framing means (FB) pertain to at least one individual interface for disassembling the frame structure of the signal to be received through the interface,

characterized in that

- the transmission unit (TRU) also includes decryption means (EB) for decryption of the signal received through the interface, said means being located in such a way that in the reception direction they are located after the de-framing means.

5

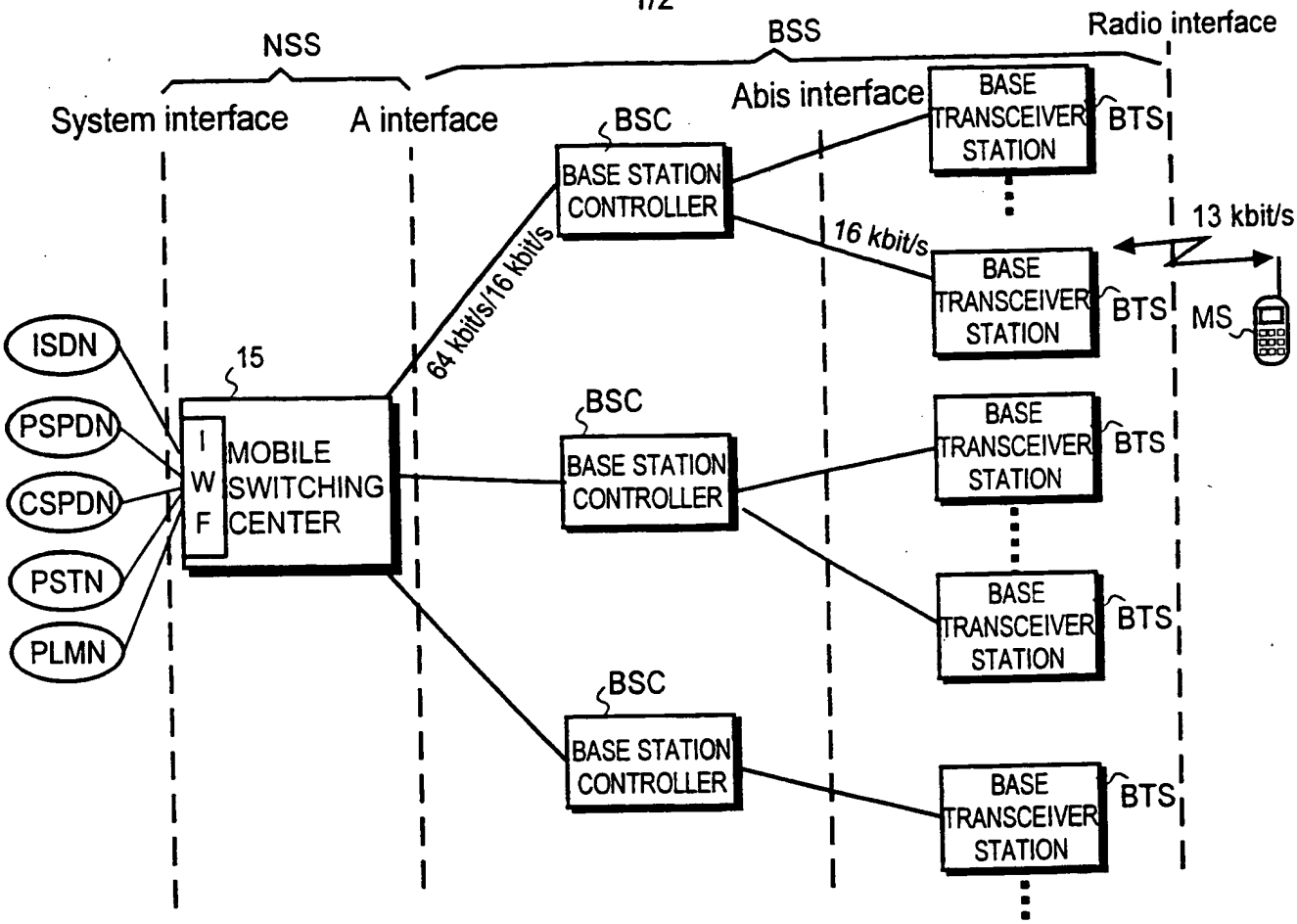


FIG. 1

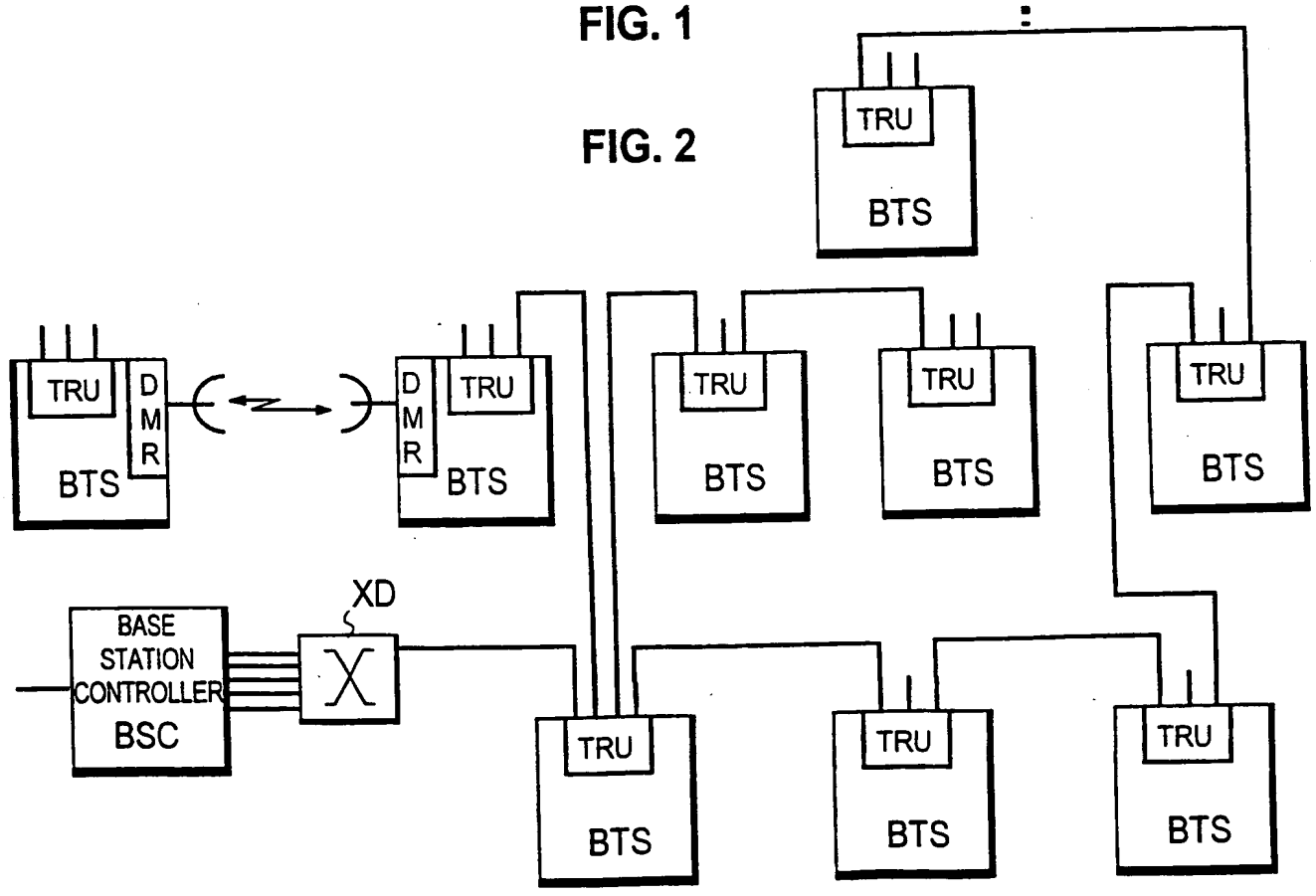


FIG. 2

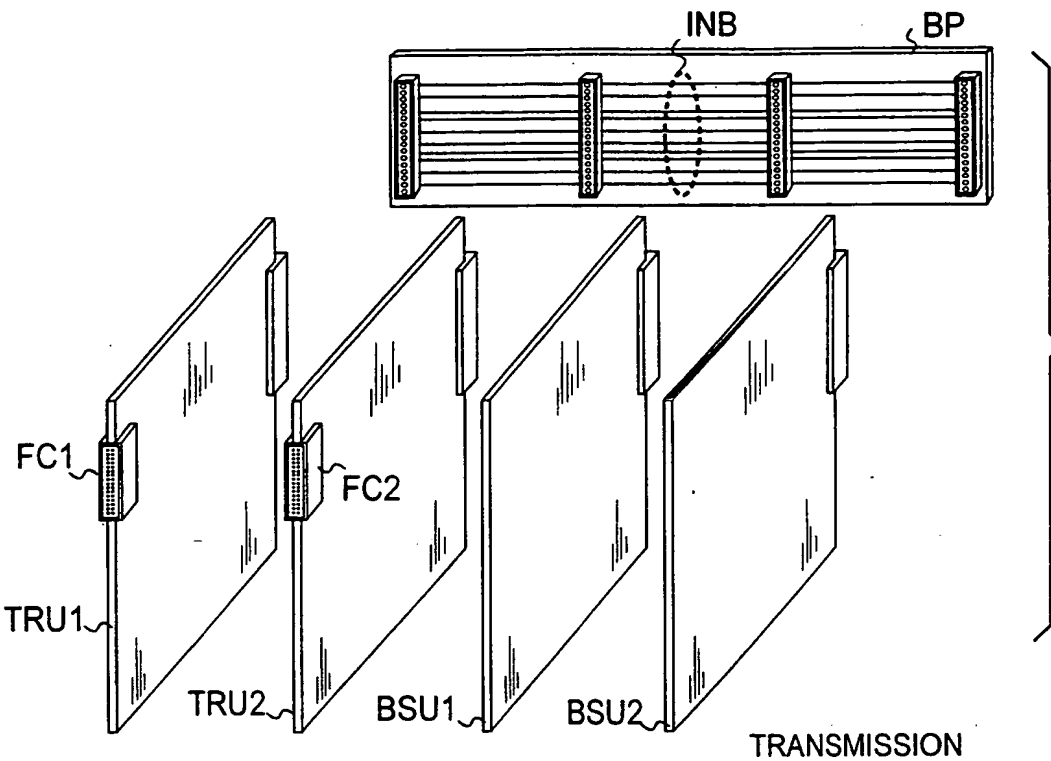

INB
BP
FC1
FC2
TRU1
TRU2
BSU1
BSU2

FIG. 3

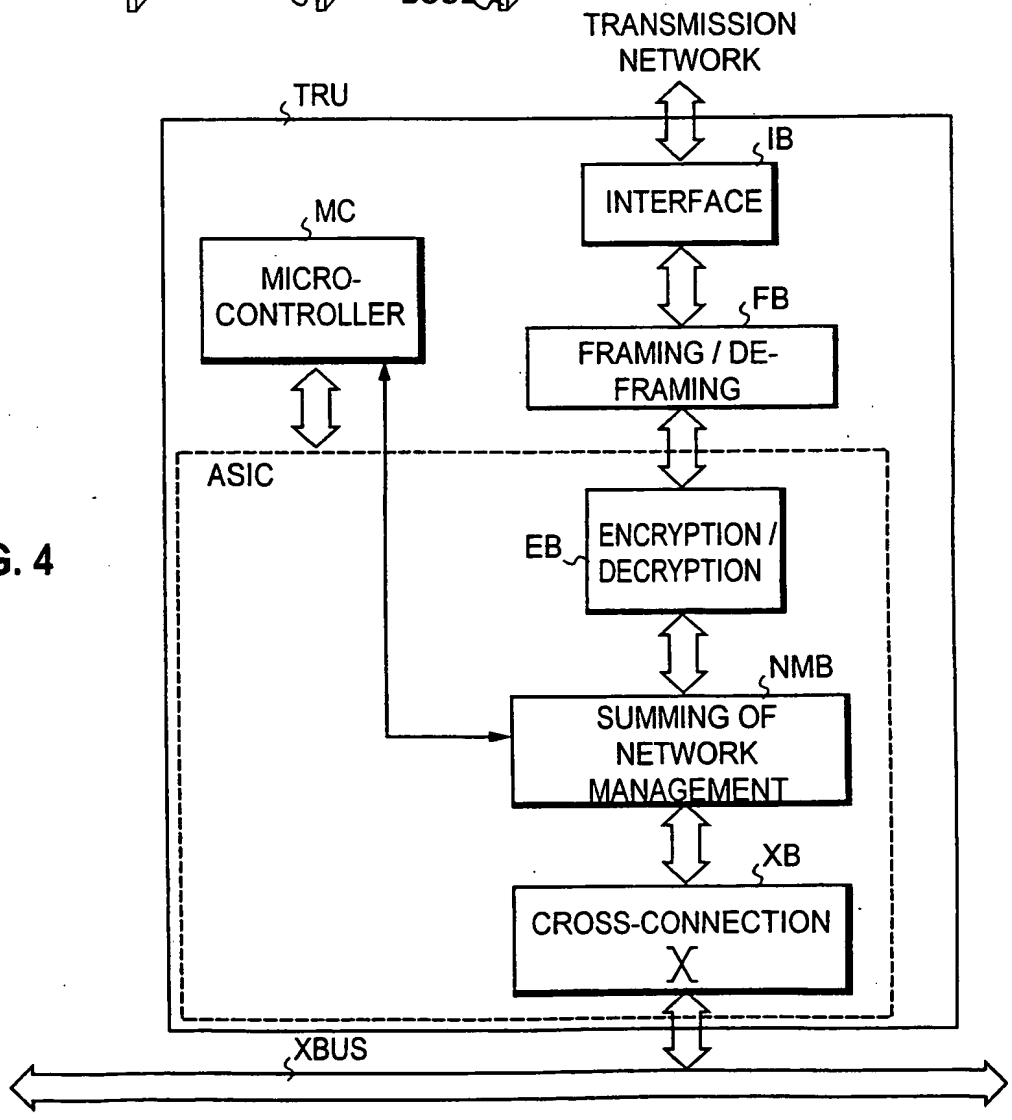

TRANSMISSION NETWORK
TRU
IB
INTERFACE
MC
MICRO-CONTROLLER
FB
FRAMING / DE-FRAMING
ASIC
EB
ENCRYPTION / DECRYPTION
NMB
SUMMING OF NETWORK MANAGEMENT
XB
CROSS-CONNECTION
X
XBUS

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/00079

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04Q 7/30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04Q, H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPIL, EDOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5077794 A (STEVEN C. TAYLOR), 31 December 1991 (31.12.91), figure 2, see the whole document ---	1-10
A	US 4771458 A (RICHARD W. CITTA ET AL), 13 Sept 1988 (13.09.88), abstract ---	6
A	EP 0093525 A1 (BRITISH TELECOMMUNICATIONS), 9 November 1983 (09.11.83), abstract --- --------	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw douhts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 July 1999	15 -07- 1999
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Malin Gullstrand/mj Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/FI 99/00079

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5077794 A	31/12/91	CA 2029248 A,C	17/05/91
US 4771458 A	13/09/88	US 4876718 A	24/10/89
		US 4944006 A	24/07/90
EP 0093525 A1	09/11/83	SE 0093525 T3	
		AT 15964 T	15/10/85
		CA 1209664 A	12/08/86
		JP 58202644 A	25/11/83

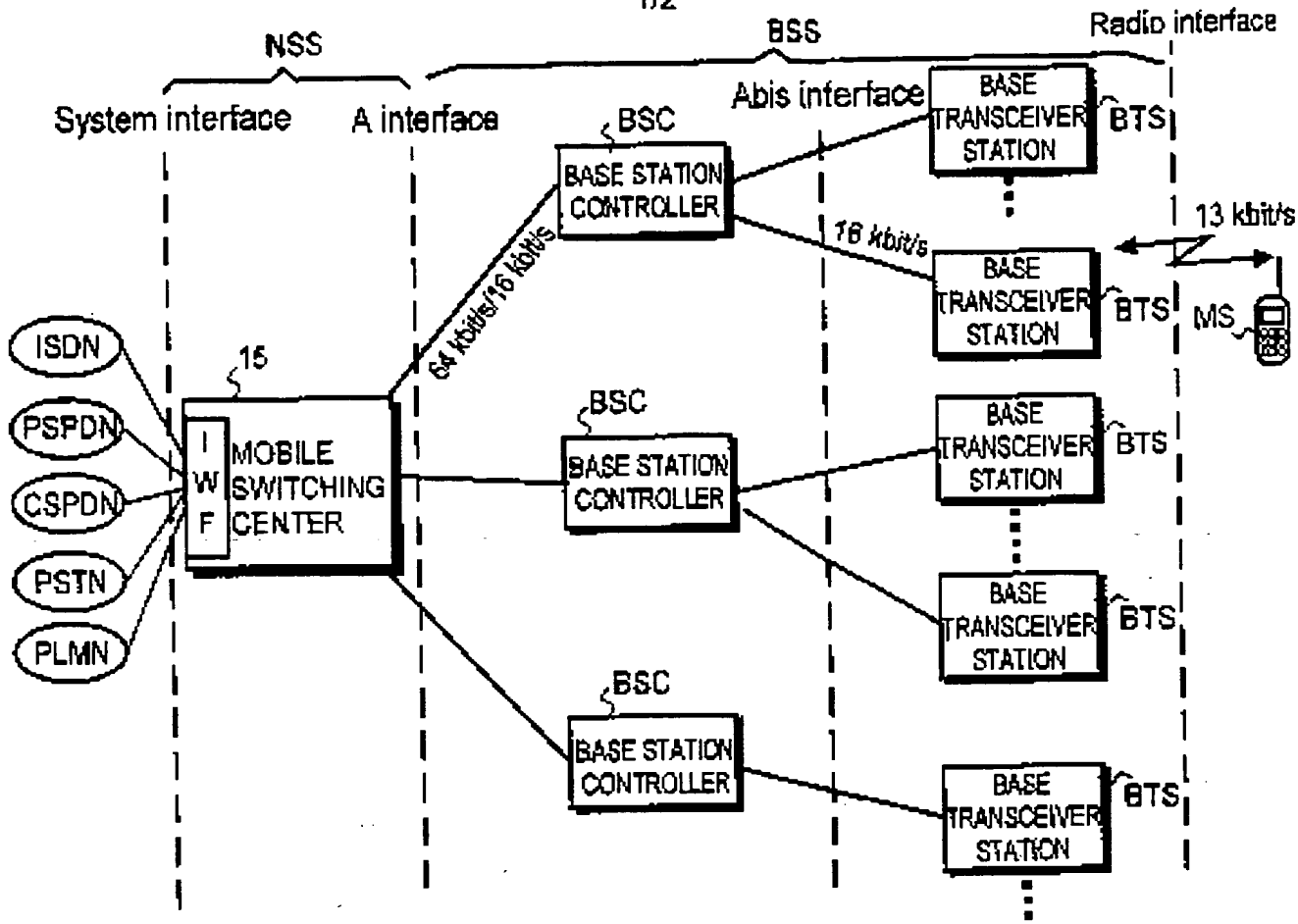

NSS
BSS
Radio interface
System interface
A interface
Abis interface
BSC
BASE STATION CONTROLLER
BASE TRANSCEIVER STATION
BTS
13 kbit/s
16 kbit/s
64 kbit/s/16 kbit/s
MS
ISDN
PSPDN
CSPDN
PSTN
PLMN
15
I W F
MOBILE SWITCHING CENTER

FIG. 1

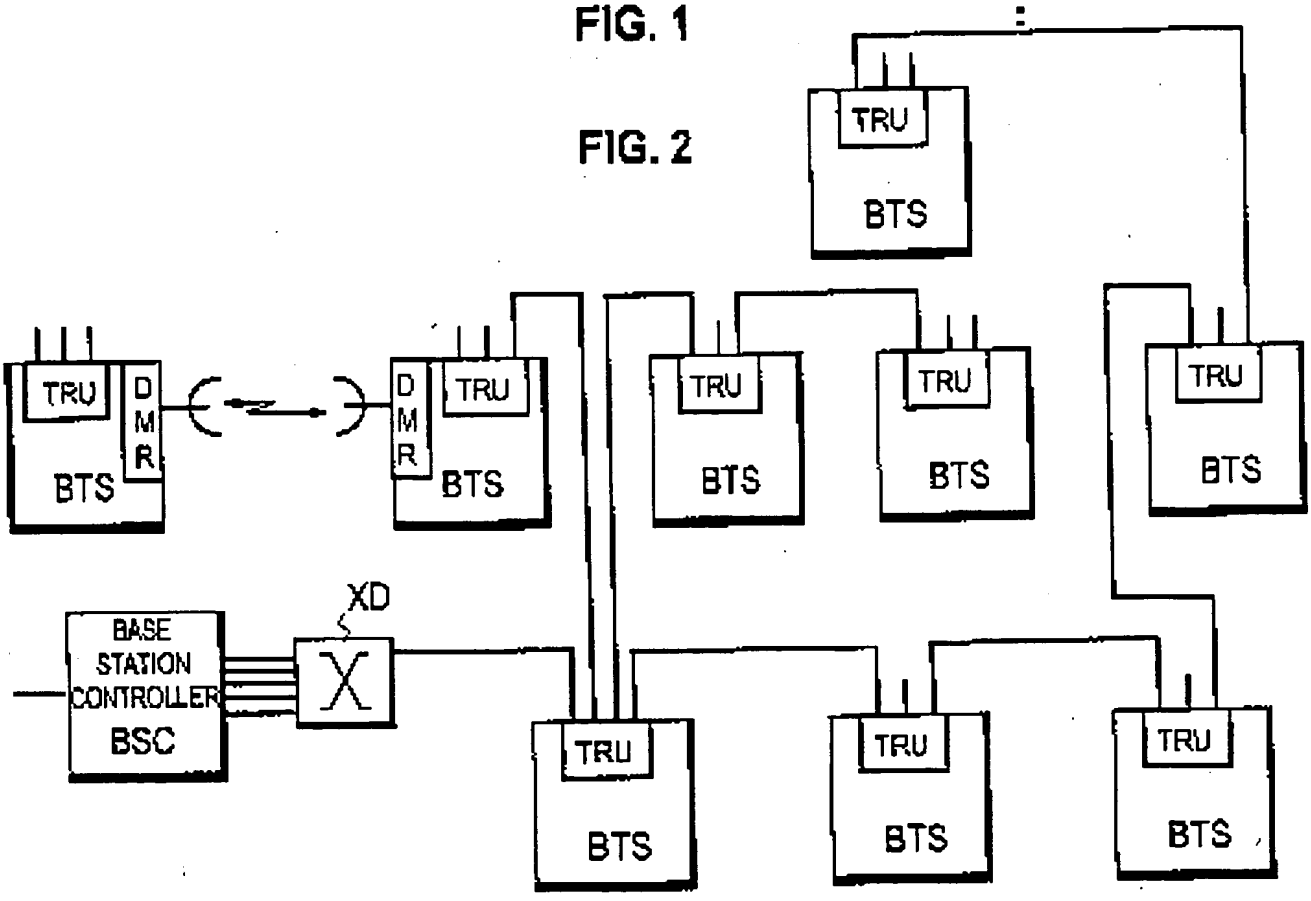

TRU
BTS
D M R
XD
BASE STATION CONTROLLER
BSC
X

FIG. 2

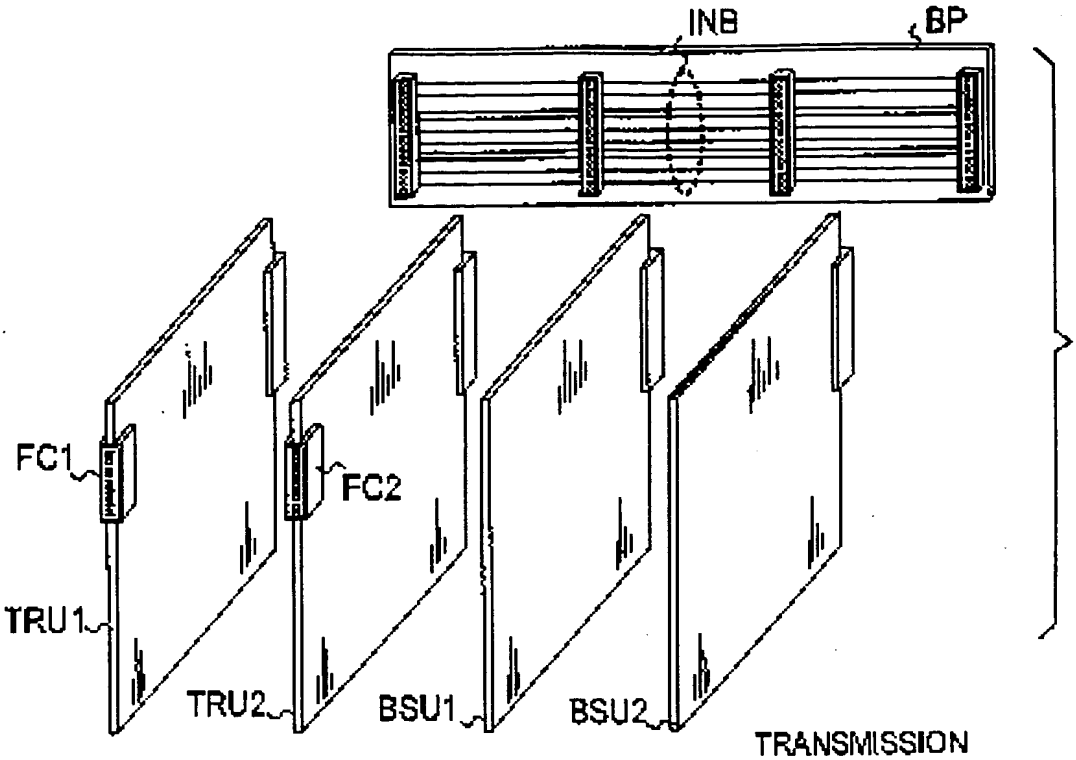


FIG. 3

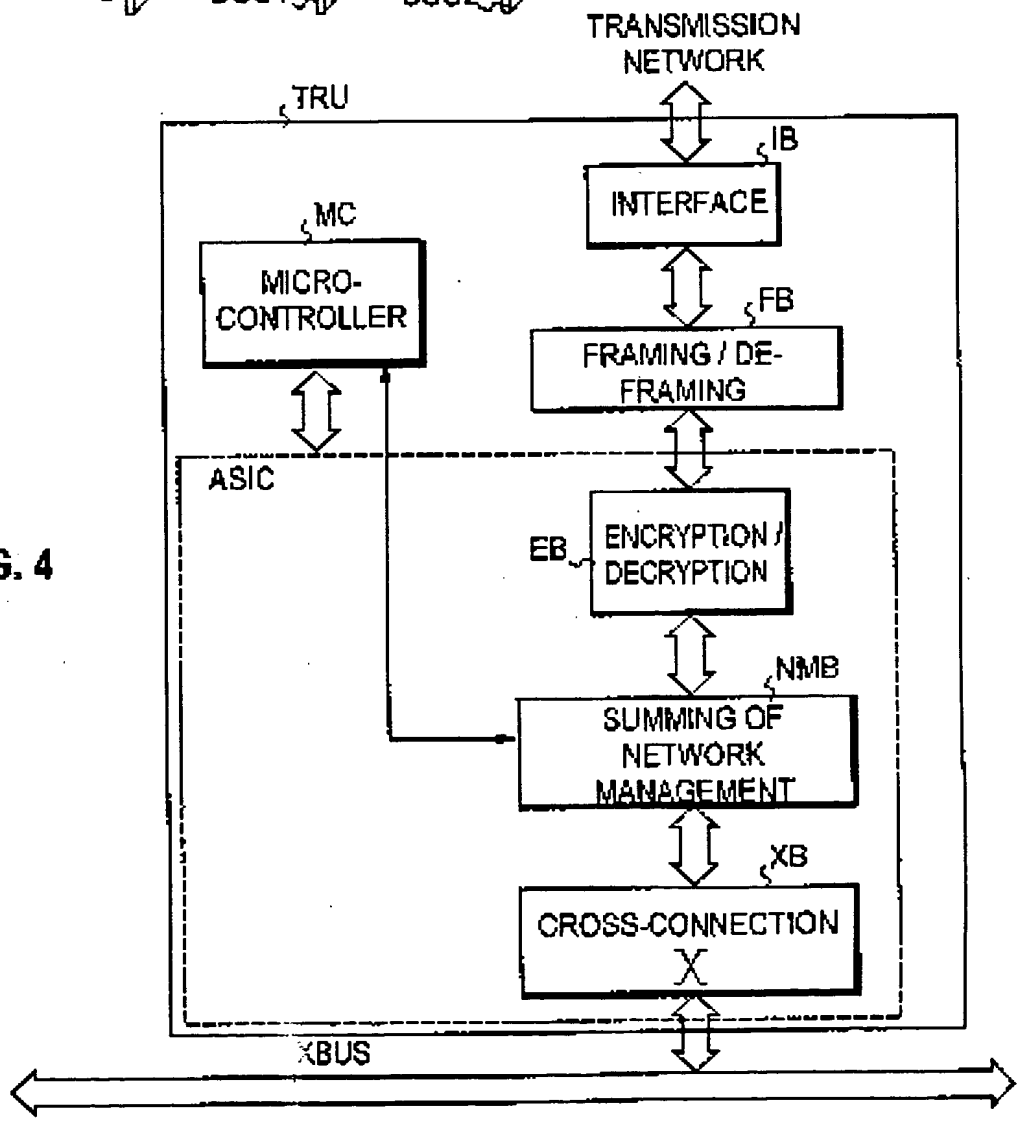


FIG. 4